Kay Bailey Hutchison, Chairman
Bill Hughes, Staff Director

347 Russell Senate Office Building
Washington, DC 20510
202-224-2946
http://rpc.senate.gov

SENATE REPUBLICAN POLICY COMMITTEE

Legislative Notice

No. 64 June 24, 2008

H.R. 6304 – FISA Amendments Act of 2008

Calendar No. 827

H.R. 6304 was read twice and placed on the Calendar on June 20, 2008.

Noteworthy

- H.R. 6304 is an original bill substantially in the form of S. 2248, which passed the Senate on February 12, 2008 by a vote of 68-29. It is a negotiated compromise that addresses the most significant Democratic concerns with S. 2248.

- Like S. 2248, it provides that the Attorney General (AG) and the Director of National Intelligence (DNI) may jointly authorize the targeting of persons reasonably believed to be located outside the United States for up to one year. Unlike S. 2248, it requires prior court review of certifications and procedures used, but with safeguards that permit immediate action where necessary to ensure that no important intelligence may be lost.

- Rather than excluding surveillances targeted at persons reasonably believed to be located outside the United States from FISA's definition of "electronic surveillance" as in S. 2248, this bill uses complex rules of construction to achieve substantially the same effect.

- Like S. 2248, it reiterates that FISA constitutes the exclusive means by which electronic surveillance and surveillance of domestic communications may be conducted, and requires prior court approval for surveillance of U.S. citizens who are overseas. But unlike S. 2248, it requires express statutory authorization for all electronic surveillance, which in some situations may constitute an impermissible encroachment on Article II powers of the President under the Constitution.

- It provides a mechanism for retroactive immunity for carriers alleged to have participated in the President's Terrorist Surveillance Program (TSP) upon certification by the AG that certain requirements have been met. The certifications may be reviewed under a "substantial evidence" standard. It also provides prospective immunity.

- The bill's provision for foreign targeting authority sunsets on December 31, 2012.

- H.R. 6304 passed in the House on June 20, 2008 by a vote of 293-129.[1]

[1] The yeas included 105 Democrats and 188 Republicans.

Background/Overview

FISA[2] was designed to trace the contours of 4th Amendment protections—establishing procedures for court orders where the Constitution seemed to require it. But rather than focus on the *persons* who could claim constitutional protection under *Katz v. United States*[3] and its progeny, FISA focused instead on the technology they used (radio- or wire-communications) and the physical location of the surveillance equipment. It requires prior court approval for activities falling into any one of four categories of "electronic surveillance"—a term defined in Section 101(f) that in effect defines the scope of FISA.

Because the underlying technology was evolving fast, with no end in sight, there was little chance that the factors defining FISA's coverage would remain stable. For this reason, the meaning of "electronic surveillance" as defined in FISA—and therefore the scope of the statute itself—has drifted with technological change since 1978. In particular, the distinction that existed between radio and wire communications in 1978, critical to ensuring that FISA would operate as intended, has been lost with the modern revolution in telecommunications. Most international and domestic telecommunications nowadays are a seamless mix of both radio and wire communications.

After the attacks of September 11, 2001, the President instituted what came to be known as the Terrorist Surveillance Program (TSP). The administration based the TSP on the President's inherent constitutional authority to conduct surveillance of foreign enemies outside the United States.

The existence of the TSP was revealed in December 2005, triggering great controversy. The controversy had not been resolved a year later when the Attorney General announced in a January 17, 2007 letter to Congress that a judge of the FISA Court had authorized the surveillance contemplated in the TSP "where there is probable cause to believe one of the communicants is a member or agent of al Qaeda or an associated terrorist group" and that such surveillance would now be conducted subject to FISA Court approval.

On April 12, 2007, in response to a congressional request, the DNI submitted a legislative proposal that would address the intelligence challenges arising under FISA in a manner consistent with the Constitution. The DNI's proposal was a comprehensive reform aimed at making the scope of FISA technology-neutral and therefore stable in its meaning.

While this proposal was being considered, it became known at the end of May 2007 that another judge of the FISA Court had issued a ruling which, according to the DNI, severely limited collection of critical communications of foreign terrorists and diverted NSA analysts from their counterterrorism mission to providing information to the Court, thus degrading the government's counterterrorism capabilities.

[2] In its original version FISA provided both immunity to telecommunications carriers that were required to assist the government and—in certain cases specifically *excluding* terrorists—a procedure and authority for warrantless surveillance.

[3] 389 U.S. 347 (1967), overruling *Olmstead v. United States*, 277 U.S. 438 (1928).

The DNI urged Congress to act quickly, and on August 4, 2007, it passed the Protect America Act of 2007 (PAA), which grants the AG and DNI authority to acquire foreign intelligence information concerning persons outside the United States for one year. The PAA was set to sunset February 1, 2008.

On October 26, the Senate Select Committee on Intelligence (SSCI) reported S. 2248. The SSCI chose not to fix the inherent problems in FISA by making its definition of "electronic surveillance" technology-neutral, electing instead to carve out of the old definition of "electronic surveillance" any surveillance targeted at persons reasonably believed to be outside the United States, and provide a warrantless procedure for such surveillance. The procedures also required FISA Court approval of collection on U.S. persons overseas for the first time in history. The SSCI bill also provided retroactive and prospective immunity from civil suits to certain telecommunications carriers.

At the end of January 2008, the PAA sunset of February 1 was extended to February 15 to permit passage of S. 2248. On February 12, 2008 the Senate passed S. 2248 by a vote of 68 to 29, but the House Democratic leadership subsequently refused to bring it up for a vote. The PAA expired on February 15, 2008. The DNI/AG certifications remain in effect until approximately August, but targets not identified in those certifications cannot be added. The Intelligence Community has said that if Congress does not act now to update FISA, then sometime this summer it will have to begin the process of seeking individualized FISA court orders on foreign targets—the same scenario that led to significant intelligence gaps and that created the need for the PAA last summer.

After lengthy discussions led by the ranking member of the SSCI, the majority leader of the House of Representatives, and executive branch officials, an agreement was reached on a FISA reform bill acceptable to all parties. The compromise bill, H.R. 6304, passed the House on June 20, 2008 on a vote of 293-129.

Highlights

H.R. 6304 contains four titles:

- Title I includes, in section 101, a new Title VII of FISA that provides a procedure for the DNI and AG jointly to authorize surveillance targeted at persons reasonably believed to be located outside the United States. A requirement of prior court review is tempered with "exigent circumstances" exceptions and safeguards that permit immediate action where necessary to ensure that no important intelligence may be lost. Section 102 contains a statement that FISA is the exclusive means for electronic surveillance, and requires express statutory authorization for future electronic surveillances. Section 103 provides for reports to Congress. Sections 104 to 109 streamline FISA procedures and contain certain technical amendments to FISA. Section 110 brings proliferators of Weapons of Mass Destruction (WMD) within the definition of those against whom the broadest categories of FISA surveillance may be conducted.

- S. 2248 clarified some of the ambiguity that has crept into the scope of FISA because of changing technology since 1978 by removing from FISA's definition of "electronic surveillance" any surveillance targeted at persons reasonably believed to be located outside the U.S. and conducted pursuant to the new warrantless certification procedure. H.R. 6304 accomplishes the same effect as S. 2248 through several different "rules of construction" found in the new Title VII.

- Title II, "Protections for Electronic Communication Service Providers," provides, in Section 201, retroactive immunity from civil suits involving intelligence activity authorized by the President under the Terrorist Surveillance Program between September 11, 2001 and January 17, 2007 (TSP), upon request of the Attorney General. Federal district courts must review the certifications requesting immunity to ensure their compliance with the requirements set forth in this bill (under a "substantial evidence" standard). This title also provides prospective immunity for carriers who cooperate with the intelligence community pursuant to strictly defined requests, and preempts state investigations of the federal government's intelligence collection activities under FISA.

- Title III, "Review of Previous Actions," provides that the Inspector General of each of the elements of the Intelligence Community that participated in the TSP shall conduct an investigation of those activities and release a coordinated report within one year.

- Title IV provides for severability, conforming amendments, and transition procedures, as well as a sunset of December 31, 2012. The sunset applies to the new FISA Title VII (the foreign targeting procedure set forth in Section 101) but not to the statement of exclusive means (Section 102) or any other part of H.R. 6304.

Bill Provisions

Section 1. Short Title; Table of Contents

TITLE I—FOREIGN INTELLIGENCE SURVEILLANCE

Section 101. Additional Procedures Regarding Certain Persons Outside the United States. Consists of three subsections:

(a) In General. This section amends FISA by adding a new Title VII.[4] The new FISA Title VII consists of eight sections:

> *Section 701. Definitions.* This section defines "Electronic Communications Service Provider," among other terms.

[4] Because communications may be acquired both during live transmission and while they are stored on physical media, circumstances that correspond to two separate titles of FISA (Titles I and III, respectively) the authority provided by this Act is set forth in a title of its own—a new Title VII. The new title replaces a Title VII consisting of technical provisions unrelated to the subject matter of this bill.

Section 702. Procedures for targeting certain persons outside the United States other than United States Persons. The key operative provision of H.R. 6304, this section provides a procedure whereby the Attorney General (AG) and Director of National Intelligence (DNI) may jointly authorize the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information for up to one year. The provision has twelve subsections:

(a) Authorization—creates the authority.

(b) Limitations—provides several safeguarding limitations. The authority cannot be used to target:

- any person "known at the time" to be located in the U.S.;
- any person who is outside the U.S. if the purpose is to target a "particular, known person" in the U.S. (so-called "reverse targeting");
- any person who is a U.S. person reasonably believed to be located outside the U.S;
- any communication in which the sender and all intended recipients are known to be located in the U.S.; or
- in any manner inconsistent with the 4th Amendment to the Constitution.

(c) Conduct of Acquisition—requires that any acquisition authorized under subsection (a) be certified under subsection (g) and comply with the procedural safeguards provided in subsections (d) and (e). This subsection also provides for:

- an "exigent circumstances" exception which allows acquisitions to begin without prior court review under subsection (i); and
- a "rule of construction" that excludes from the traditional FISA Court order requirement all acquisitions targeted in accordance with this Title at persons reasonably believed to be located outside the U.S.

(d) Targeting Procedures—requires special procedures to ensure that targeted persons are reasonably believed to located outside the U.S. subject to judicial review under subsection (i).

(e) Minimization Procedures—requires the AG to adopt "minimization procedures" and makes the procedures subject to judicial review. The term "minimization procedures" refers to a series of procedures governing the acquisition, retention, or dissemination of information pertaining to U.S. persons, consistent with the need to disseminate foreign intelligence information.[5]

[5] Most existing "minimization procedures" have been mandatory within the intelligence community for decades pursuant to applicable directives. The procedures are designed to protect the identity and other private information of U.S. persons that is not foreign intelligence information.

(f) Guidelines for Compliance with Limitations—requires the AG to adopt guidelines to ensure compliance with the limitations to the Title VII certification authority.

(g) Certification—Specifies that before the § 702(a) authority may be exercised, the AG and DNI must makes a series of certifications, including:

- the targeting and minimization procedures to be used have been approved or will be submitted to the FISA Court for approval;
- the AG has adopted the guidelines contemplated in subsection (f);
- the procedures used will comply with the 4th Amendment to the Constitution;
- that a significant purpose of the acquisition is to obtain foreign intelligence information;
- that an electronic communications service provider is participating in the acquisition; and
- the acquisition complies the with the limitations in subsection (b).

(h) Directives and Judicial Review of Directives—empowers the AG and DNI to require electronic communication service providers to provide the information authorized for collection under Title VII. This subsection also provides for recourse to the FISA courts for enjoining (or enforcing) the directives.

- This subsection provides immunity to electronic service providers who comply with directives under this subsection.

(i) Judicial Review of Certifications and Procedures—provides extensive procedures for prior judicial review of the certifications under subsection (a) and the targeting and minimization procedures adopted in connection with the certification, subject to the "exigent circumstances" exception and safeguards to protect intelligence information under subsection (c).

- The government may appeal an adverse order to the FISA Court of Review. Relevant surveillances may continue during the pendency of any such appeal.

(j) Judicial proceedings—sets forth procedural provisions.

(k) Maintenance and Security of Records and Proceedings—provides record-keeping for documents and proceedings under Title VII, including statements of reasons for decisions of the FISA courts thereunder.

(l) Assessments and Reviews—provides for extensive review, oversight, and reporting by the Department of Justice, the Director of National Intelligence, and agency heads, as well as review and oversight by the FISA Court and Congress.

Section 703. Certain Acquisitions inside the United States Targeting United States Persons Outside the United States. This section permits acquisitions conducted **inside** the U.S. of the communications of U.S. persons outside the U.S. only upon a FISA Court order finding of "probable cause" that the target is a foreign power, or agent, officer, or employee of a foreign power. The procedure is similar to that put in place by the original FISA, but is more streamlined.

- Contains a "rule of construction" that excludes such acquisitions from the traditional FISA Court order requirement of FISA Title I.

- Provides for emergencies.

- Gives immunity to electronic service providers required to provide assistance under this section.

Section 704. Other Acquisitions Targeting United States Persons Outside the United States. This section permits acquisitions conducted **outside** the U.S. of the communications of U.S. persons outside the U.S. only upon a FISA Court order finding of "probable cause" that the target is a foreign power, or agent, officer, or employee of a foreign power. The procedure is substantially similar to that of Section 703 (and hence also to the procedures of the original FISA) but here the FISA Court has no jurisdiction to review the means by which the acquisition is to be conducted.

- Contains a "rule of construction" that excludes such acquisitions from the traditional FISA Court order requirement of FISA Title I.

- Provides for emergencies.

- Gives immunity to electronic service providers required to provide assistance under this section.

Section 705. Joint Applications and Concurrent Authorizations. Provides for situations where the acquisition of the communications of a U.S. person outside the U.S. is proposed to be conducted both inside the U.S. and outside the U.S.

Section 706. Use of information acquired under Section 703. This section makes public disclosure and use in criminal proceedings of the information acquired pursuant to Title VII subject to the same provisions as specified in Title I, except for the provision in subsection (j) relating to notice following emergency authorization.

Section 707. Congressional Oversight. This section provides for semiannual reports to the Intelligence and Judiciary Committees of the House and Senate on the implementation of Title VII.

Section 708. Savings Provision. Provides that nothing in Title VII shall be construed to limit the government's authority under any other title of FISA.

(b) Table of Contents.

(c) Technical and Conforming Amendments. This subsection contains changes to 18 U.S.C. § 2511(2)(a)(ii)(B), which sets forth elements of the exception to the federal criminal law prohibition against unauthorized wiretaps for electronic service providers who assist the government pursuant to FISA.

Section 102. Statement of exclusive means by which electronic surveillance and interception of domestic communications may be conducted. This section states that FISA and specific provisions in title 18 of the criminal code are the exclusive means by which "electronic surveillance" and the interception of domestic wire, oral, or electronic communications may be conducted. Only an "express statutory authorization"—other than an amendment to FISA or title 18—may constitute additional exclusive means. This latter provision is intended to prevent any future justification of warrantless surveillance on the basis of the Authorization to Use Military Force[6] and similar authorizations. This provision does not sunset, and may constitute an impermissible encroachment on Article II powers of the president under the Constitution.

Section 103. Submittal to Congress of certain court orders under the Foreign Intelligence Surveillance Act of 1978. This section expands reporting to Congress by requiring copies of FISA Court orders, decisions, and opinions that contain a significant interpretation of FISA, which are to be provided on a new accelerated timetable.

Sections 104 through 108. FISA Streamlining. These largely technical provisions are meant to increase the speed and efficiency of the FISA process. Included in these changes are: an extension of time (up to 7 days) for emergency authorizations under traditional FISA and allowance for the Deputy Director of the FBI to certify FISA applications.

Section 109. Foreign Intelligence Surveillance Court. This section streamlines Section 103 of FISA, which establishes the FISA Court and Court of Review, by

- relaxing one of the restrictions on the composition of the FISA Court;
- making it easier to have hearings and rehearings of the FISA Court sitting *en banc* (the full court rather than just one judge); and
- providing some flexibility during the pendency of appellate proceedings, including appeals to the Supreme Court.

Section 110. Weapons of mass destruction. This section brings proliferators of WMD within FISA's "foreign power/non-US person agent of a foreign power" definitions, thereby making them subject to the broadest sweep of authorities under FISA. This provision largely mirrors the WMD section in S. 2248, but includes a narrower definition of "weapons of mass destruction."

[6] September 18, 2001.

TITLE II—PROTECTIONS FOR ELECTRONIC COMMUNICATION SERVICE PROVIDERS

This title provides immunity to electronic communication service providers alleged to have provided assistance to the government under the President's Terrorist Surveillance Program until its termination on January 17, 2007 (TSP) and under FISA Court orders thereafter.

Section 201. Procedures for Implementing Statutory Defenses under the Foreign Intelligence Surveillance Act of 1978. This section creates a new FISA Title VIII, consisting of four sections:

Section 801. Definitions.

Section 802. Procedures for Implementing Statutory Defenses. This section provides immunity from civil actions for telecommunication service providers, upon certification by the Attorney General that a specific provider did or did not participate in the TSP. Review is limited to the validity of the Attorney General's certification under a "substantial evidence" standard. It allows parties to participate in briefing legal arguments, but limits the materials that the court may review in order to safeguard national security. Specifically, the court may review the letters or directives that were given to the providers by the government in conjunction with the TSP. Under this section:

- courts cannot examine whether providers acted "in good faith" in complying with the government's requests for assistance under the TSP;
- courts cannot examine the legality of the TSP;
- service providers who cooperated with the TSP will not be forced to defend against frivolous claims; and
- the identities of those providers who cooperated with the TSP will not be publicly disclosed.

Section 803. Preemption. This section preempts state proceedings and investigations involving service providers.

Section 804. Reporting.

Section 202. Technical amendments.

TITLE III—REVIEW OF PREVIOUS ACTIONS

Section 301. Review of Previous Actions. This section requires Inspector General investigations of the President's Terrorist Surveillance Program in each of the relevant elements of the Intelligence Community. It cannot duplicate other reviews that have been or are being conducted and does not permit review of the substance of the pertinent legal opinions.

TITLE IV—OTHER PROVISIONS

Section 401. Severability.

Section 402. Effective Date. This section provides that the effective date shall be the date of enactment.

Section 403. Repeals. This section provides, *inter alia*, that the new Title VII sunsets on December 31, 2012.

Section 404. Transition Procedures.

Administration Position

As of the publication of this notice, no Statement of Administration Position (SAP) had been released. By letter to the Speaker of the House of Representatives dated June 19, 2008, the AG and DNI expressed strong support for H.R. 6304.

Possible Amendments

As of the publication of this notice, there is no unanimous consent agreement limiting the consideration of amendments.